(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 326 157 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
09.07.2003 Bulletin 2003/28

(51) Int Cl.[7]: **G06F 1/00**

(21) Application number: **02258536.8**

(22) Date of filing: **11.12.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SI SK TR
Designated Extension States:
AL LT LV MK RO

(30) Priority: **12.12.2001 US 339634 P**
12.02.2002 US 74804
31.05.2002 US 159537

(71) Applicant: **Pervasive Security Systems Inc.**
Menlo Park, California 94025 (US)

(72) Inventor: **Garcia, Denis Jacques Paul**
Palo Alto, CA 94306 (US)

(74) Representative: **Ablett, Graham Keith et al**
Ablett & Stebbing,
Caparo House,
101-103 Baker Street
London W1U 6FQ (GB)

(54) Method and apparatus for securing digital assets

(57) The present invention relates to digital assets which are in a secured form that only those with granted access rights can access. Even with the proper access privilege, when a secured file is classified, at least a security clearance key is needed to ensure those who have the right security clearance can ultimately access the contents in the classified secured file. According to one embodiment, a secured file or secured document includes two parts: a header, and an encrypted data portion. The header includes security information that points to or includes access rules, a protection key and a file key. The access rules facilitate restrictive access to the encrypted data portion and essentially determine who the secured document can be accessed. The file key is used to encrypt/decrypt the encrypted data portion and protected by the protection key. If the contents in the secured file are classified, the file key is jointly protected by the protection key as well as a security clearance key associated with a user attempting to access the secured file.

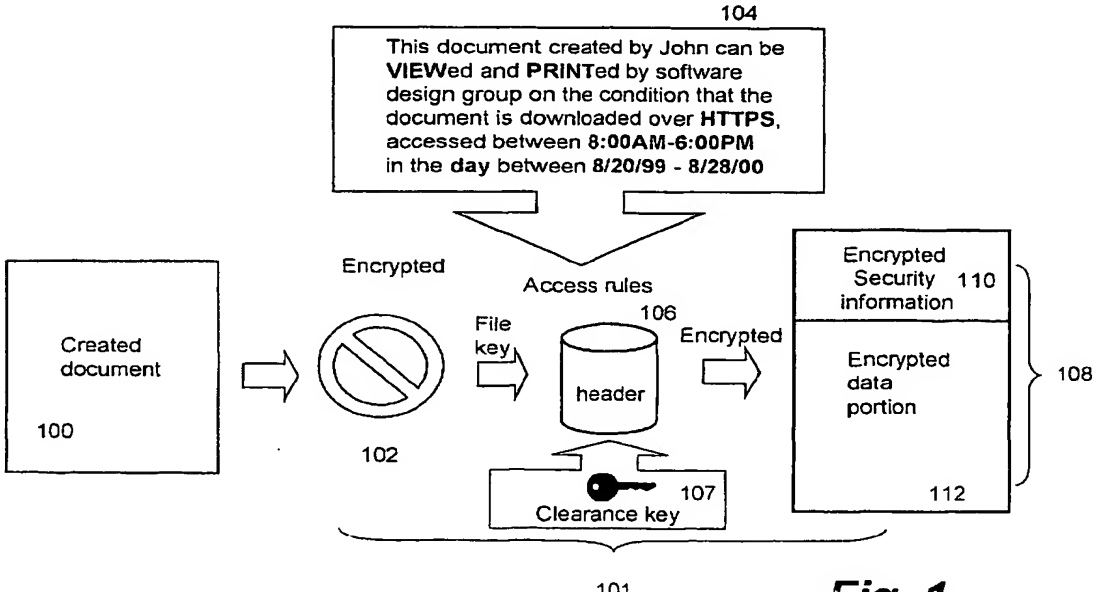


Fig. 1

EP 1 326 157 A2

assets are in a secured form that only those with granted access rights can access. Even with the proper access privilege, when a secured file is classified, at least a security clearance key is needed to ensure those who have the right security clearance can ultimately access the contents in the classified secured file.

[0010] In another aspect of the present invention, the format of the secured file is so designed that the security information stays with the file being secured at all times or pointed to by a pointer in the file. According to one embodiment, a secured file or secured document includes two parts: an attachment, referred to as a header, and an encrypted document or data portion. The header includes security information that points to or includes access rules, a protection key and a file key. The access rules facilitate restrictive access to the encrypted data portion and essentially determine who/how and/or when/where the secured document can be accessed. The file key is used to encrypt/decrypt the encrypted data portion and protected by the protection key. If the contents in the secured file are classified, the file key is jointly protected by the protection key as well as a security clearance key associated with a user attempting to access the secured file. As a result, only those who have the proper access privileges are permitted to obtain the protection key, jointly with the security clearance key, to retrieve the file key to encrypt the encrypted data portion.

[0011] In still another aspect of the present invention, the security clearance key is generated and assigned in accordance with a user's security access level. A security clearance key may range from most classified to non-classified. If a user has the need to access a secured file classified with a certain security or confidential level, a corresponding security clearance key with that security level is assigned therefor. In one embodiment, a security clearance key with a security level is so configured that the key can be used to access secured files classified at or lower than the security level. As a result, a user needs to have only one security clearance key. In still another aspect of the present invention, multiple auxiliary keys are provided when a corresponding security clearance key is being requested. The security clearance key is the one being requested, generated in accordance with the determined security level and can be used to facilitate the access to a secured file classified at a corresponding security or confidentiality level. The auxiliary security clearance keys are those keys generated to facilitate access to secured files classified respectively less than the corresponding security or confidentiality level. Depending on implementation, the security clearance key(s) may be further protected by means of secondary authentication, such as biometric information verification or a second password, to increase security level of the security clearance key(s).

[0012] Depending on implementation and application, the present invention may be implemented or employed in a client machine and a server machine. Typically, if a user's access privilege (i.e., access rights) to a secured file is locally determined in a client machine, the present invention may be implemented as an executable module configured to operate locally, preferably, in an operating system running in the client machine. If a user's access right to a secured file is remotely determined in a server machine, the present invention may be implemented as an executable module configured to operate in the server machine as well as in the client machine.

[0013] Objects, features, and advantages of the present invention will become apparent upon examining the following detailed description of an embodiment thereof, taken in conjunction with the attached drawings.

[0014] These and other features, aspects, and advantages of the present invention will become better understood with regard to the following description, appended claims, and accompanying drawings where:

FIG. 1 shows a diagram of securing a created document according to one exemplary secured file form used in the present invention;

FIG. 2A shows a diagram of what is referred to herein as a two-pronged access scheme according to one embodiment of the present invention;

FIG. 2B shows a flowchart of a process for granting a proper security clearance level (i.e., a clearance key) according to one embodiment of the present invention;

FIG. 2C shows a diagram of generating a clearance key according to one embodiment of the present invention;

FIG. 2D shows a diagram of generating a clearance key according to another embodiment of the present invention;

FIG. 3A illustrates an exemplary structure of a secured file according to one embodiment of the present invention;

FIG. 3B shows an exemplary header structure of a secured file according to one embodiment of the present invention;

FIG. 4 there is shown a flowchart of process for accessing a secured document according to one embodiment of the present invention and may be understood in conjunction with FIG. 3A and FIG. 3B;

FIG. 5 shows a flowchart of a process for securing a file or document being created according to one embodiment of the present invention; and

FIG. 6 shows an exemplary implementation of the present invention.

[0015] The present invention pertains to a process, a system, a method and a software product for securing electronic data or digital assets. According to one aspect of the present invention, secured files may be classified in several hierarchical security levels. To access the secured classified files, in addition to a user key, a user is assigned a clearance key that is based on at least two complementary concepts, "Need to Know" and "Sensi-

who and/or how the document 100, once secured, can be accessed. In some cases, the access rules 104 also determine or regulate when or where the document 100 can be accessed. In addition, security clearance information 107 is added to the header 106 if the secured file 108 is classified. In general, the security clearance information 107 is used to determine a level of access privilege or security level of a user who is attempting to access the contents in the secured file 108. For example, a secured file may be classified as "Top secret", "Secret", "Confidential", and "Unclassified".

[0025] According to one embodiment, the security clearance information 107 includes another layer of encryption of the file key with another key referred to herein as a clearance key. An authorized user must have a clearance key of proper security level in addition to an authenticated user key and proper access privilege to retrieve the file key. As used herein, a user key or a group key is a cipher key assigned to an authenticated user and may be used to access a secured file or secure a file, or create a secured file. The detail of obtaining such a user key upon a user being authenticated is provided in US Patent Application No.:10/074,804.

[0026] According to another embodiment, the security clearance information 107 includes a set of special access rules to guard the file key. The retrieval of the file key requires that the user passes an access rule measurement. Since access privilege of a user may be controlled via one or more system parameters (e.g., a policy), the access rule measurement can determine if the user has sufficient access privilege to retrieve the file key in conjunction with the corresponding user key. With the detailed description to follow, those skilled in the art can appreciate that other forms of the security clearance information 107 may be possible. Unless otherwise specified, the following description is based on the security clearance information 107 being another layer of encryption with one or more clearance keys.

[0027] In accordance with the security clearance information 107, a user may be assigned a hierarchical security clearance level based on, perhaps, a level of trust assigned to the user. A level of trust implies that one user may be more trusted than another and hence the more trusted user may access more classified files. Depending on implementation, a level of trust may be based on job responsibility of the user or a role of the user in a project or an organization background checks, psychological profiles, or length of service, etc. In any case, a level of trust assigned to the user augments additional aspect to the access privilege of the user such that the user must have proper security clearance to access a classified secured file even if the user is permitted by the access rules to access the file.

[0028] As will be further described in detail below, unless the level of security clearance of the user permits, a secured classified file (i.e., the file that is both secured and classified) may not be accessed even if the user has an authenticated user (or group) key and permitted by the access rules in the secured classified file. In one embodiment, the level of security clearance of the user is determined by one or more clearance keys assigned thereto. In general, a clearance key permits a user to access a secured file classified as "top secret", the same clearance key may permit the user to access all secured files classified less secure, such as "secret" or "confidential", where it has been assumed that the user has proper access privilege to be granted by the access rules in the file. In one embodiment, a clearance key is further secured by means of secondary authentication, such as biometric information verification and a second password. In other words, a clearance key may not be automatically released to or activated for a user upon an authenticated login, unless the user provides additional information.

[0029] In general, a header is a file structure, preferably small in size, and includes, or perhaps links to, security information about a resultant secured document. Depending on an exact implementation, the security information can be entirely included in a header or pointed to by a pointer that is included in the header. According to one embodiment, the access rules 104, as part of the security information, are included in the header 106. The security information further includes the file key and/or one or more clearance keys, in some cases, an off-line access permit (e.g. in the access rules) should such access be requested by an authorized user. The security information is then encrypted by a cipher (i.e., an en/decryption scheme) with a user key associated with an authorized user to produce encrypted security information 110. The encrypted header 106, if no other information is added thereto, is attached to or integrated with the encrypted data portion 112 to generate the resultant secured file 108. In a preferred embodiment, the header is placed at the beginning of the encrypted document (data portion) to facilitate an early detection of the secured nature of a secured file. One of the advantages of such placement is to enable an access application (i.e., an authoring or viewing tool) to immediately activate a document securing module (to be described where it deems appropriate) to decrypt the header if permitted. Nevertheless, there is no restriction as to where the encrypted header 106 is integrated with the encrypted data portion 112.

[0030] It is understood that a cipher may be implemented based on one of many available encryption/decryption schemes. Encryption and decryption generally require the use of some secret information, referred to as a *key*. For some encryption mechanisms, the same key is used for both encryption and decryption; for other mechanisms, the keys used for encryption and decryption are different. In any case, data can be encrypted with a key according to a predetermined cipher (i.e., encryption/decryption) scheme. Examples of such schemes may include, but not be limited to, Data Encryption Standard algorithm (DES), Blowfish block cipher and Twofish cipher. Therefore, the operations of

[0036] FIG. 2D shows a diagram of generating a clearance key according to another embodiment of the present invention. The key generator 244 receives one or more parameters 242 controlling the security level determined at 226 of FIG. 2B to generate a number of sets of alphanumeric or binary numbers as a primary key 246 and auxiliary keys 247. The primary key 246 is the one being requested, generated in accordance with the determined security level and can be used to facilitate the access to a secured file classified at a security or confidentiality level. The auxiliary keys 247 are those keys generated to facilitate the access to secured files classified less than the security or confidentiality level. As shown in the figure, it is assumed that the primary key 246 is for accessing a secured file classified at level 2. Accordingly, the auxiliary keys 247 can be respectively used to access secured files classified level 3, level 4, ... to level N, all less than level 2 in terms of security or confidentiality. To facilitate the description of the present invention, the following description is based on FIG. 2C and can be readily applied to FIG. 2D.

[0037] Returning to FIG. 2B, after a proper clearance key is generated at 228, the clearance key is associated with the account at 230 so that the user will use the correct key to access a secured file that requires a clearance key. The process 220 now awaits any call for the clearance key at 232. Depending on implementation, the clearance key may be stored locally or remotely and retrievable only when there is a need for it to access a classified secured file. In some cases, the clearance key can only be retrievable when a user passes a secondary authentication means. For example, a user is entitled to access certain secured files classified at least at a securily level. The clearance key associated with the user may be configured to be protected by means of secondary authentication, such as biometric information verification or a second password, to increase security level of the clearance key. When a non-secured classified file is accessed, the clearance key is not needed and therefore will not be released to or activated for the user. When a secured classified file is accessed, the process 220 goes to 234, wherein the clearance key is released to the user to facilitate the retrieval of the file key in the secured file, provided the user has furnished necessary information or passed secondary authentication if needed.

[0038] FIG. 3A illustrates an exemplary structure of a secured file 300 including a header 302 and an encrypted data portion 304. Depending on implementation, the header 302 may or may not include a flag or signature 306. In one case, the signature 306 is used to facilitate the detection of the security nature of a secured file among other files. The header 302 includes a file key block 308, a key block 310 and a rule block 312. The file key block 308 includes a file key 309 that is encrypted by a cipher with a protection key 320 (i.e., a doc-key key sometimes) and further with the clearance key 322 associated with a user who attempts to access the secured file 300. Alternatively, the file 309 is encrypted with the clearance key 322 and then the protection key 320. The protection key 320 is encrypted and stored in the key block 310. In general, the key block 310 has an encrypted version of the protection key 320 and can be only accessible by designated user(s) or group(s). There may be more than one key blocks in a header, wherein three key blocks are shown in FIG. 3A. To recover or retrieve the protection key 320, a designated user must have proper access privilege to pass an access rule test with the embedded access rules in the rule block 312.

[0039] All access rules are encrypted with a user key (e.g., a public user key) and stored in the rule block 312. A user attempting to access the secured file uses must have a proper user key (e.g., a private user key) to decrypt the access rules in the rule block 312. The access rules are then applied to measure the access privilege of the user. If the user is permitted to access the secured file in view of the access rules, the protection key 320 in the key block 310 is retrieved to retrieve the file key 309 so as to access the encrypted data portion 304. However, when it is detected that the secured file is classified, which means that the file key can not be retrieved with only the protection key, the user must posses a clearance key. Only does the user have the clearance key, together with the retrieved protection key 320, the file key 309 may be retrieved to proceed with the decryption of the encrypted data portion 304.

[0040] According to one embodiment, the encrypted data portion 304 is produced by encrypting a file that is non-secured. For example, a non-secured document can be created by an authoring tool (e.g., Microsoft Word). The non-secured document is encrypted by a cipher with the file key. The encryption information and the file key are then stored in the security information.

[0041] According to another embodiment, the non-secured document (data) is encrypted using the following aspects, a strong encryption using a CBC mode, a fast random access to the encrypted data, and an integrity check. To this end, the data is encrypted in blocks. The size of each block may be a predetermined number or specific to the document. For example, the predetermined number may be a multiple of an actual encryption block size used in an encryption scheme. One of the examples is a block cipher (i.e., a type of symmetric-key encryption algorithm that transforms a fixed-length block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length. This transformation takes place under the action of a cipher key (i.e., a file key). Decryption is performed by applying the reverse transformation to the ciphertext block using another cipher key or the same cipher key used for encryption. The fixed length is called the block size, such as 64 bits or 128. Each block is encrypted using a CBC mode. A unique initiation vector (IV) is generated for each block.

[0042] Other encryption of the non-secured data can be designed in view of the description herein. In any

public key or together with a clearance key associated with the user if a subject secured file is secured. Now instead of retrieving the protection key after the access rules are successfully measured against access privilege of the user attempting to access a secured file, the protection key is retrieved first with a user's private key. The protection key can be used to retrieve the access rules that are subsequently used to measure against the access privilege of the user if the protection key was used to encrypt the access rules. If the user is permitted to access the contents in the file, the file key is then retrieved with the protection key (or together with the clearance key). Alternatively, right after the protection key is retrieved, the protection key (or together with the clearance key) is used to retrieve the file key. The file key is then to retrieve the access rules that are subsequently used to measure against the access privilege of the user. In any case, if the user is determined that the user has sufficient access privilege in view of all access policies, if there are any, the retrieved file key can be used to continue the description of the encrypted data portion.

[0051] FIG. 4 there is shown a flowchart of process 400 for accessing a secured document according to one embodiment of the present invention and may be understood in conjunction with FIG. 3A or FIG. 3B. The process 400 may be implemented in an executable module (e.g., document securing module) that can be activated when a user intends to access a secured document. For example, a user is using a client machine running a Microsoft Windows operating system to access a secured document stored in a folder, a local, or remote store. By activating a Window Explorer or Internet Explorer, the user may display a list of files, some are non-secured and others are secured. Among the secured files, some of them are classified and secured in the manner in accordance with FIG. 3A. Within the display of the list of files, a desired one can be selected. Alternatively, a desired file may be selected from an application, for example, using "open" command under File of Microsoft Word application.

[0052] In any case, at 402, such desired document is identified to be accessed. Before proceeding with the selected document, the process 400 needs to determine whether the selected file is secured or non-secured. At 404, the selected document is examined. In general, there are at least two ways to examine the secure nature of the selected document. A first possible way is to look for a flag or signature at the beginning of the document. As described above, in some secured documents, a flag, such as a set of predetermined data, is placed in the header of a secured document to indicate that the document being accessed is secured. If no such flag is found, the process 400 goes to 420, namely, the selected documented is assumed non-secured and thus allowed to pass and load to a selected application or place desired by the user. A second possible way is to look for a header in a selected document. Being a secured document, there is a header attached to an encrypted data portion. The data format of the header shall be irregular in comparison with the selected document if it is non-secured. If it is determined that the selected document has no irregular data format as required by a selected application, the process 400 goes to 420, namely, the selected document is assumed to be non-secured and thus allowed to pass and load to a selected application or place desired by the user.

[0053] Now if it is determined at 404 that the selected document is indeed secured, the process 400 goes to 406, wherein the user and/or the client machine being used by the user are checked to determine if the user and/or the client machine are authenticated. The details of the user authenticating himself/herself/itself may be provided in US Patent Application No.:10/074,804. In the case that the user and/or the client machine are not authenticated, the process 400 goes to 418 that may display an appropriate error message to the user. It is now assumed that the user and/or the client machine are authenticated, the header or security information therein is decrypted with the authenticated user key.

[0054] At 408, the access rules in the decrypted security information are retrieved. As described above, there may be sets of access rules, each set designated for a particular user or members of a particular group. With the authenticated user key and/or a corresponding user identifier, a corresponding set of access rules is retrieved. At 410, the retrieved access rules are compared to (or measured against) the access privileges associated with the user. If the measurement fails, which means that the user is not permitted to access this particular document, a notification or alert message may be generated to be displayed to the user at 418. If the measurement passes successfully, which means that the user is permitted to access this particular document, the process 400 moves on to decrypt and retrieve the protection key at 411 and then determine if the secured document is classified at 412. When it is determined that the secured document is not classified or there is no security clearance requirement in the security information, the process 400 goes to 416, wherein a file key is retrieved and, subsequently, used to decrypt the encrypted data portion in the selected (secured) document. When it is determined that the secured document is classified, the process 400 goes to 414 that checks if the authenticated user possesses a clearance key matching the security clearance requirement. In general, the security level of the clearance key must be equal to or higher than the security clearance requirement in the secured classified document. If the security level of the clearance key is not sufficient enough, the process 400 goes to 418 that can be configured to display an appropriate error message to the user. If the security level of the clearance key is sufficient enough, the process 400 goes to 416.

[0055] In any case, a file key is retrieved with the protection key alone if the secured document is not classi-

decryption schemes may be readily used, if desired.

[0064] According to one embodiment, the client module 202 is analogous in many ways to a device driver that essentially converts more general input/output instructions of an operating system to messages that a device/module being supported can understand. Depending on the OS in which the present invention is implemented, the client module 602 may be implemented as a VxD (virtual device driver), a kernel or other applicable format.

[0065] In operation, the user selects a document that is associated with an application 606 (e.g., MS WORD, PowerPoint, or printing). The application 606 acts on the document and calls an API (e.g., createFile, a Common Dialog File Open Dialog with Win32 API in MS Windows) to access the installable file system (IFS) manger 612. If it is detected that an "Open" request is made from the application 206, the request is passed to an appropriate file system driver (FSD) 614 to access the requested document. When it is detected that the requested document is secured, the key store 209 and the cipher module 610 are activated and an authenticated user (private) key is retrieved. The encrypted security information in the header of the requested secure document is decrypted with the user key. Now the access rules in the secured document are available, a rules measurement is carried out in the client module 602 to determine if the user is permitted to access the selected secured document. If the measurement is successful, that means the user is permitted to access the secured document, a file key is retrieved from the security information with a retrieved protection key as well as the clearance key and, subsequently, the cipher module 610 proceeds to decrypt the encrypted document (i.e., the encrypted data portion) in the client module 602. The clear contents are then returned to the application 606 through the IFS manager 612. For example, if the application 606 is an authoring tool, the clear contents are displayed. If the application 606 is a printing tool, the clear contents are sent to a designated printer.

[0066] In another embodiment, an operating system (OS) access, known as the ProcessID property, can be used to activate an application (as an argument to the AppActivate method). The parameter ProcessID identifies the application and an event handler thereof takes necessary parameters to continue the OS access to the Installable File System (IFS) Manager 612 that is responsible for arbitrating access to different file system components. In particular, the IFS Manager 612 acts as an entry point to perform various operations such as opening, closing, reading, writing files and etc. With one or more flags or parameters passed along, the access activates the client module 602. If the document being accessed by the application is regular (non-secured), the document will be fetched from one of the File System Driver (FSD) (e.g., FSD 614) and passed through the client module 602 and subsequently loaded into the application through the IFS Manager 612. On the other hand, if the document being accessed by the application is secured, the client module 602 activates the key store 609 and the cipher module 610 and proceeds to obtain an authenticated user key to retrieve the access rules therein. Pending the outcome from the access test module 609, a file key may be retrieved to decrypt the encrypted data portion of the secured document by the cipher in the cipher module 610. As a result, the data portion or the document in clear mode will be loaded into the application through the IFS Manager 612.

[0067] The present invention has been described in sufficient details with a certain degree of particularity. It is understood to those skilled in the art that the present disclosure of embodiments has been made by way of examples only and that numerous changes in the arrangement and combination of parts may be resorted without departing from the spirit and scope of the invention as claimed. Accordingly, the scope of the present invention is defined by the appended claims rather than the foregoing description of embodiments.

Claims

1. In a system for providing restrictive access to electronic data, wherein the electronic data is structured in a format that controls access to contents in the electronic data, the format comprising:-

   a header including security information controlling the access to the contents in the electronic data, wherein the security information includes at least a first key and a second key, the second key is used to encrypt the first key, the second key is encrypted and the encrypted second key is guarded by access rules;
   an encrypted data portion generated by encrypting the electronic data with the first key according to a predetermined cipher scheme; and

   wherein the header is integrated with the encrypted data portion to generate a secured file.

2. A format according to Claim 1, wherein the access rules are displayable in an application to display access restrictions in the secured file.

3. A format according to Claim 1 or 2, wherein the access rules are further encrypted and included in the security information.

4. A format according to any preceding claim, wherein the second key is used to encrypt the first key according to the predetermined cipher scheme and the encrypted first key is protected by security clearance information controlling restrictive access to the first key.

tents in the electronic data, the method comprising:-

obtaining an authenticated user key associated with a user attempting to access the electronic data;
retrieving access rules embedded in the format to determine if the user has proper access privilege;
retrieving a second key if the user is permitted to access the electronic data;
if the content in the electronic data is classified:-

obtaining a clearance key associated with the user;
using the second key and the clearance key to ultimately retrieve a first key;

if the content in the electronic is not classified:-

using the second key to retrieve a first key;
decrypting, using the first key, an encryption data portion representing an encrypted version of the electronic data.

20. A method according to Claim 19, wherein the access rules are encrypted.

21. A method according to Claim 19 or 20, wherein the retrieving access rules comprises:-

decrypting the access rules with the authenticated user key; and
testing if access privilege of the user is within the access rules.

22. A method according to Claim 19, wherein the using of the second key and the clearance key to ultimately retrieve the first key comprises:-

obtaining the first key by sequentially using either the second key and the clearance key to decrypt an encrypted version of the first key or the clearance key and the second key to decrypt an encrypted version of the first key.

23. A software product to be executed in a computing system for providing restrictive access to electronic data, wherein the electronic data is structured in a format that controls access to contents in the electronic data, the software product comprising:-

program code for generating an encrypted data portion by encrypting the electronic data with a first key according to a predetermined cipher scheme;
program code for encrypting the first key with a second key, if the electronic data is not classified;
program code for encrypting the first key with the second key together with a clearance key, if the electronic data is classified;
program code for encrypting the second key to produce an encrypted version of the second key;
program code for applying access rules to protect the encrypted version of the second key; and
program code for integrating a header with the encrypted data portion to produce a secured file, wherein the header includes the encrypted first key, the encrypted second key and the access rules.

24. A software product to be executed in a computing system for providing restrictive access to electronic data, wherein the electronic data is structured in a format that controls access to contents in the electronic data, the software product comprising:-

program code for obtaining an authenticated user key associated with a user attempting to access the electronic data;
program code for retrieving access rules embedded in the format to determine if the user has proper access privilege;
program code for retrieving a second key if the user is permitted to access the electronic data;
if the contents in the electronic data is classified:-

program code for obtaining a clearance key associated with the user;
program code for using the second key and the clearance key to ultimately retrieve a first key;

if the contents in the electronic is not classified;

program code for using the second key to retrieve a first key;
program code for decrypting, using the first key, an encryption data portion representing an encrypted version of the electronic data.

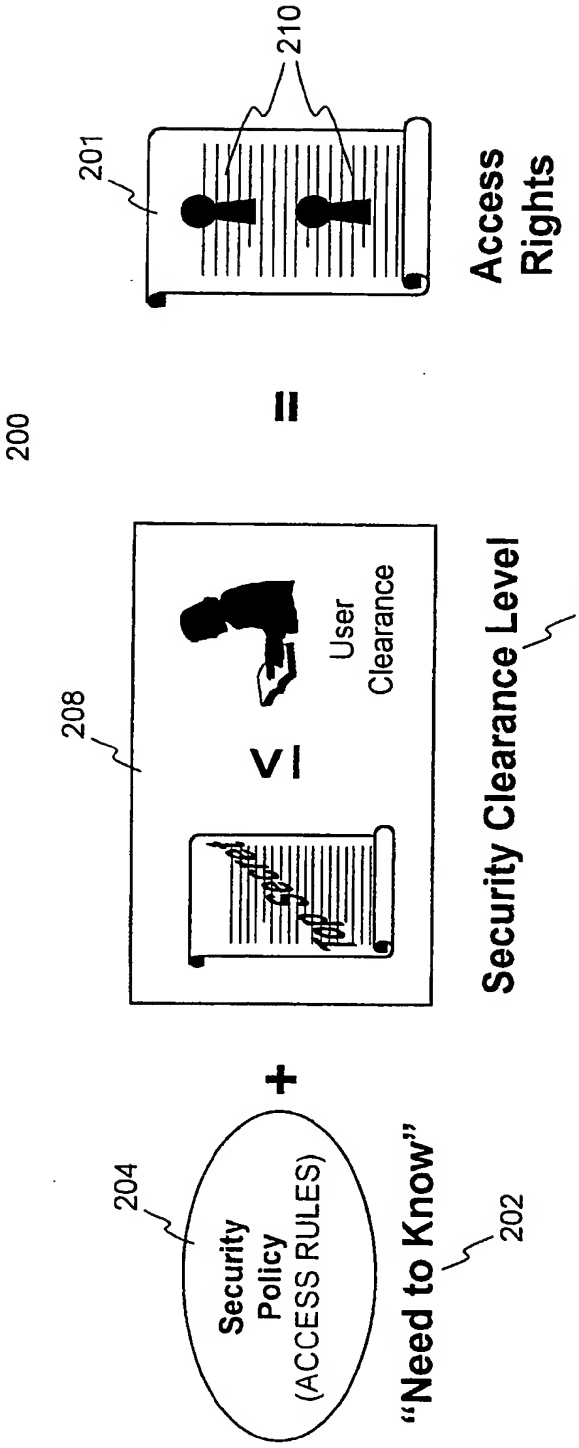

200
201
210
Access Rights
=
208
VI
User Clearance
Security Clearance Level
206
+
204
Security Policy (ACCESS RULES)
"Need to Know"
202

Fig. 2A

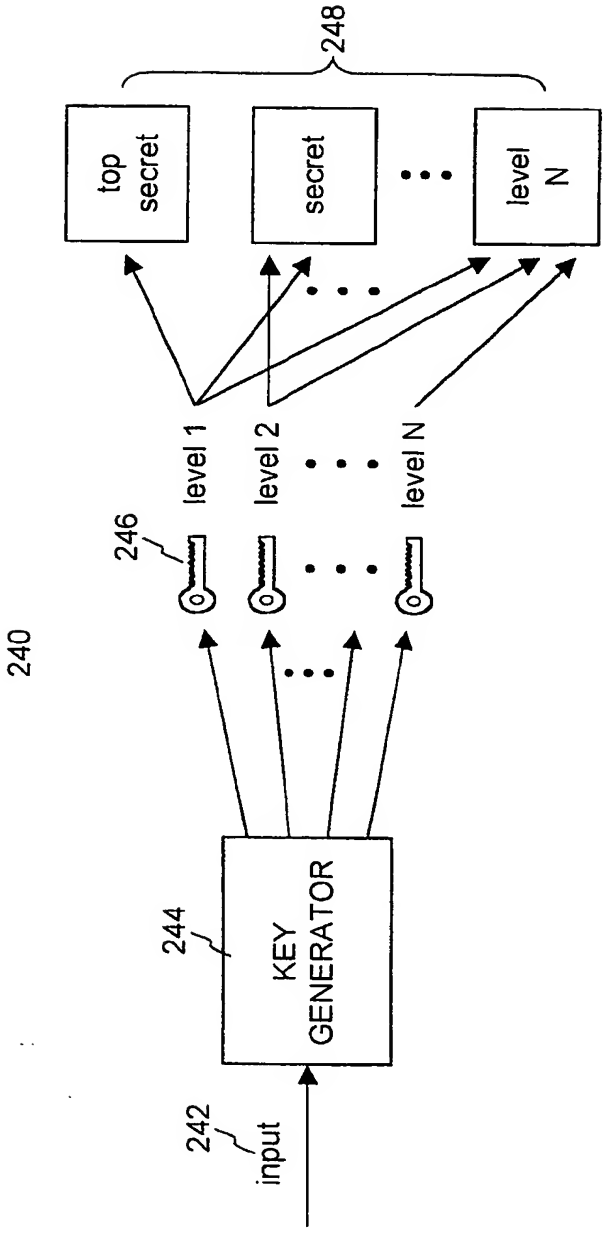

240
242
input
244
KEY GENERATOR
246
level 1
level 2
level N
248
top secret
secret
level N

Fig. 2C

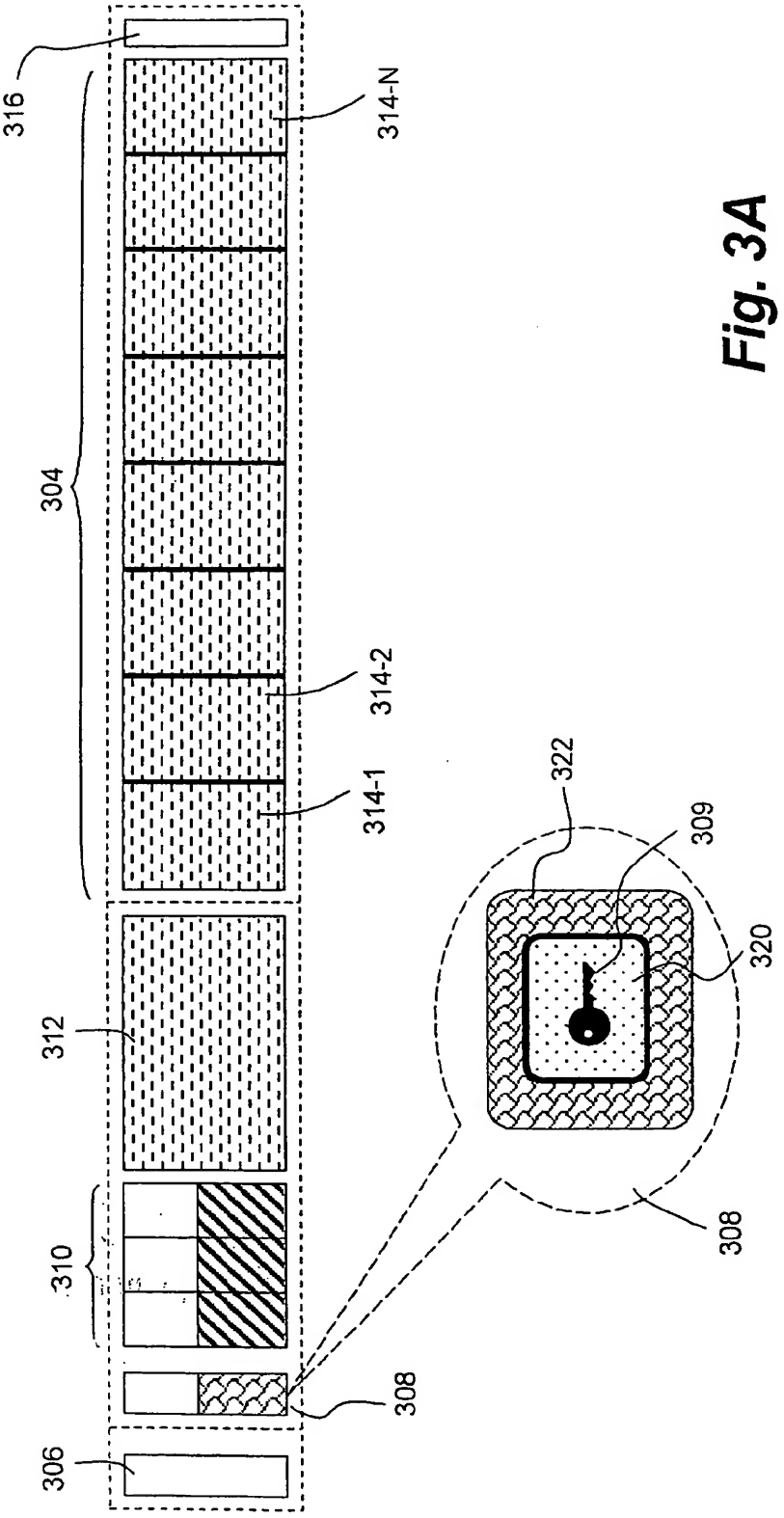
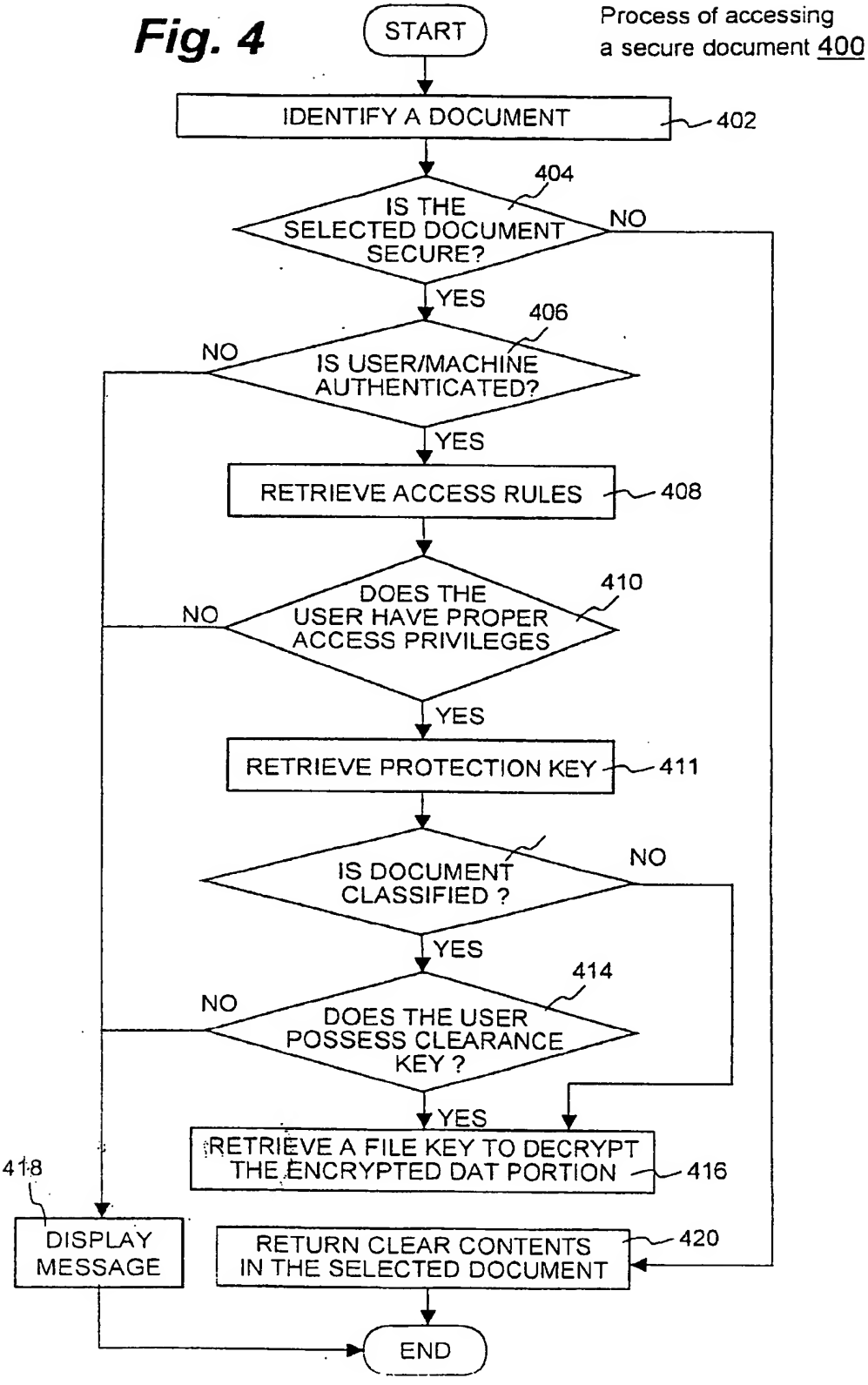


Fig. 3A

Fig. 4


START
Process of accessing a secure document 400
IDENTIFY A DOCUMENT
402
404
IS THE SELECTED DOCUMENT SECURE?
NO
YES
406
IS USER/MACHINE AUTHENTICATED?
NO
YES
RETRIEVE ACCESS RULES
408
DOES THE USER HAVE PROPER ACCESS PRIVILEGES
410
NO
YES
RETRIEVE PROTECTION KEY
411
IS DOCUMENT CLASSIFIED ?
NO
YES
414
DOES THE USER POSSESS CLEARANCE KEY ?
NO
YES
RETRIEVE A FILE KEY TO DECRYPT THE ENCRYPTED DAT PORTION
416
418
DISPLAY MESSAGE
RETURN CLEAR CONTENTS IN THE SELECTED DOCUMENT
420
END

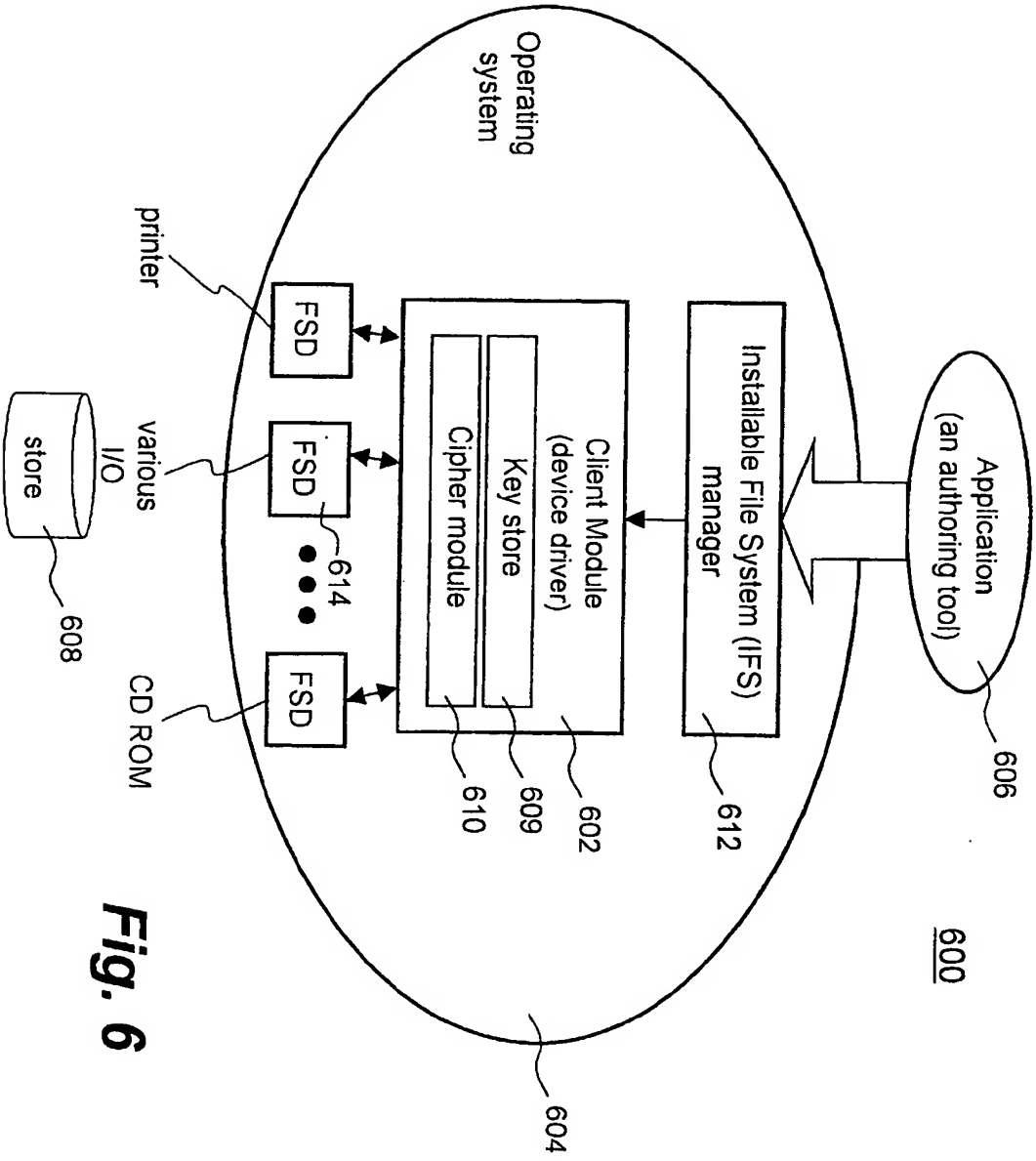

Application
(an authoring tool)
606
600
Installable File System (IFS)
manager
612
Operating
system
Client Module
(device driver)
Key store
Cipher module
602
609
610
604
FSD
FSD
FSD
614
printer
various
I/O
CD ROM
store
608

Fig. 6

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 326 157 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
10.12.2003 Bulletin 2003/50

(43) Date of publication A2:
09.07.2003 Bulletin 2003/28

(21) Application number: **02258536.8**

(22) Date of filing: **11.12.2002**

(51) Int Cl.[7]: **G06F 1/00**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SI SK TR
Designated Extension States:
AL LT LV MK RO

(30) Priority: **12.12.2001 US 339634 P**
12.02.2002 US 74804
31.05.2002 US 159537

(71) Applicant: **Pervasive Security Systems Inc.**
Menlo Park, California 94025 (US)

(72) Inventor: **Garcia, Denis Jacques Paul**
Palo Alto, CA 94306 (US)

(74) Representative: **Ablett, Graham Keith et al**
Ablett & Stebbing,
Caparo House,
101-103 Baker Street
London W1U 6FQ (GB)

(54) Method and apparatus for securing digital assets

(57) The present invention relates to digital assets which are in a secured form that only those with granted access rights can access. Even with the proper access privilege, when a secured file is classified, at least a security clearance key is needed to ensure those who have the right security clearance can ultimately access the contents in the classified secured file. According to one embodiment, a secured file or secured document includes two parts: a header, and an encrypted data portion. The header includes security information that points to or includes access rules, a protection key and a file key. The access rules facilitate restrictive access to the encrypted data portion and essentially determine who the secured document can be accessed. The file key is used to encrypt/decrypt the encrypted data portion and protected by the protection key. If the contents in the secured file are classified, the file key is jointly protected by the protection key as well as a security clearance key associated with a user attempting to access the secured file.

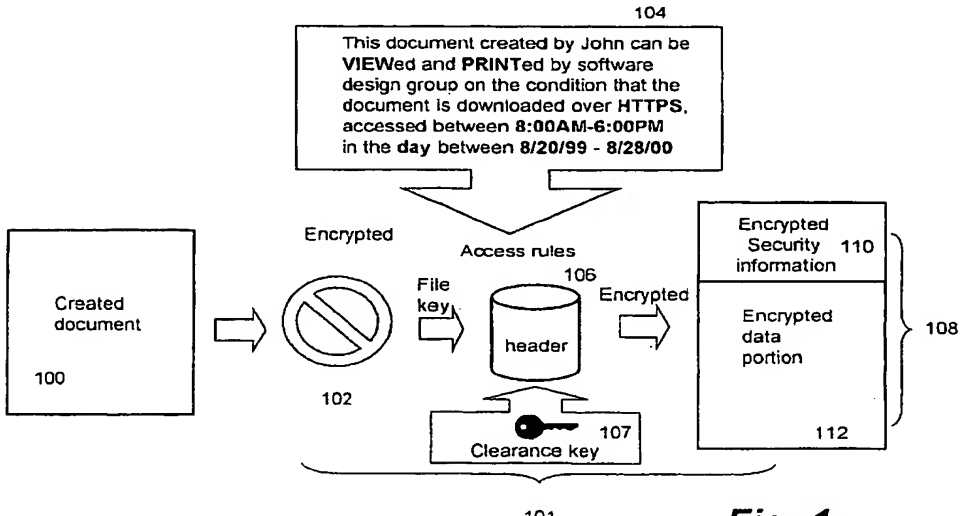


Fig. 1

EP 1 326 157 A3

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 25 8536

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

08-10-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0163387 A	30-08-2001	AU 4721301 A	03-09-2001
		WO 0163387 A2	30-08-2001
		US 2002016922 A1	07-02-2002
GB 2328047 A	10-02-1999	US 6272631 B1	07-08-2001
		DE 19827659 A1	07-01-1999
		FR 2767208 A1	12-02-1999
		JP 11085622 A	30-03-1999
		US 6389535 B1	14-05-2002
		US 6532542 B1	11-03-2003
		US 6044155 A	28-03-2000
		US 6253324 B1	26-06-2001
WO 0178285 A	18-10-2001	AU 5305801 A	23-10-2001
		EP 1277300 A1	22-01-2003
		WO 0178285 A1	18-10-2001
		US 2001029581 A1	11-10-2001
EP 0950941 A	20-10-1999	JP 11272561 A	08-10-1999
		EP 0950941 A2	20-10-1999
US 5708709 A	13-01-1998	EP 0778512 A2	11-06-1997
		JP 9288575 A	04-11-1997
EP 1154348 A	14-11-2001	CN 1324028 A	28-11-2001
		EP 1154348 A2	14-11-2001
		JP 2002033727 A	31-01-2002
		US 2001056541 A1	27-12-2001
US 5870477 A	09-02-1999	AU 7707894 A	18-04-1995
		WO 9509410 A1	06-04-1995
		JP 2000151576 A	30-05-2000